REMARKS

The Examiner is thanked for the performance of a thorough search.

STATUS OF CLAIMS

Claims 3-5, 7-8, 10, 13-14, 16, and 18-19 have been cancelled.

Claims 2, 6, 9, and 12 have been amended.

Claims 30-45 have been added.

No claims have been withdrawn.

Claims 1-2, 6, 9, 11-12, 15, 17, and 20-45 are currently pending in the application.

SUMMARY OF THE REJECTIONS/OBJECTIONS

Claims 1-5, 7-8, 10, 12-22, and 24-29 have been rejected under 35 U.S.C. § 102(e) as allegedly anticipated by U.S. Patent Application Publication Number 2005/0097317 of Trostle et al. (" *Trostle* "). Claim 6 has been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Trostle* in view of U.S. Patent Number 5.982,898 issued to Hsu et al. (" *Hsu* "). Claims 9, 11, and 23 have been rejected under 35 U.S.C. § 103(a) as allegedly unpatentable over *Trostle* in view of U.S. Patent Application Publication Number 2002/0059516 issued to Turtiainen et al. (" *Turtiainen* "). The rejections are respectfully traversed.

A. CLAIM 1

(1) INTRODUCTION TO CLAIM 1

Claim 1 features:

"A method for facilitating secure communications among multicast nodes in a telecommunications network, the method comprising the computer-implemented steps of:

receiving, from a first node, **a first request *to store an encryption key***, wherein the first request includes an ***identifier***, and wherein the first node uses the encryption key to encrypt data that is **multicast with the *identifier*** to a plurality of second nodes;

in response to the first request,

storing the encryption key;

creating and storing an association **between the *encryption key* and the *identifier***;

receiving, from at least one second node of the plurality of second nodes, **a second request *to obtain the encryption key***, wherein the second request includes the ***identifier***;

in response to the second request,

based on the *identifier* included in the second request **and the *association*** between the encryption key and the identifier, retrieving the encryption key; and

sending the encryption key to the at least one second node for use in decrypting the encrypted data." (Emphasis added.)

Thus, Claim 1 features two requests: (1) a **first request** to ***store an encryption key*** in which that first request includes an ***identifier***, and (2) a **second request** to ***obtain the encryption key*** in which that second request includes the same ***identifier*** as in the first request (e.g., because the encrypted data is **multicast with the *identifier***). Claim 1 also features **creating and storing** an ***association*** between the ***encryption key*** and the ***identifier***.

For example, in the embodiment illustrated in FIG. 2A and 2B and described in paragraphs [0035] - [0050]of the application, a multicast originator 122 can request that certificate authority server 150 store the session key for the multicast, and that request includes a session identifier among other data. The certificate authority server 150 creates and stores an association between the session key and the session identifier, such as in the form of a multicast session certificate that includes the association between the session key and the session identifier. When multicast originator 122 sends a multicast that is encrypted with the session key to multicast receivers 132, 142, the multicast includes the identifier so that multicast receivers 132, 142 can then request the session key from certificate authority server 150 by providing the identifier to the certificate authority. Once the session key is received from the certificate authority, multicast receivers 132, 142 can decrypt the multicast.

As discussed in the Background of the Application, conventional approaches for multicasts require that all the members of the multicast negotiate back and forth to obtain an

agreed upon set of encryption parameters, such as the session key to be used for the multicast. The problem for multicasts with large numbers of members is that such negotiations can be complex and lengthy. (*See* Application, page 4, paragraph [0015].) The approach of Claim 1 avoids this problem by having one node, such as the originator node, request that the session key be stored by another entity or node, such as a certificate authority (CA), and by having the CA associate the session key with an identifier. When other nodes receive the multicast that includes the identifier, those receiving nodes can obtain the session key from the CA. In order to know which key to provide in response to such a request, the CA associates the identifier with the session key, and the multicast receivers use the identifier that is communicated via the multicast to request the corresponding session key from the CA.

(2) INTRODUCTORY DISCUSSION OF *TROSTLE*

In contrast to the approach of Claim 1, *Trostle* discloses an approach for secure multicasts involving multiple multicast groups that uses a "multi-master directory" for which access control is on a per object and per attribute access basis. (Abstract.) An authentication service registers publishers and subscribers of the multicast, and the use of the multi-master directory provides a readily scalable and secure architecture. (Abstract.) *Trostle* utilizes the "multi-master directory" to address problems of typical multicast approaches that utilize a centralized group controller, such as that the single group controller represents a central point of failure and that the single group controller is a potential bottleneck in managing the group and distributing session keys. (Paragraphs [0019] and [0020].) Therefore, by using the multi-master directory in place of a centralized group controller, *Trostle* avoids the single failure and bottleneck problems of those prior approaches.

(3) THE OFFICE ACTION'S CITATIONS FROM *TROSTLE*

As a preliminary matter, the Applicant notes that the Office Action associates steps and features of the claims with paragraph numbers from the prior art without identifying which features of the cited references correspond to which features of the claims. As a result, the Applicant has had to engage in educated guesswork to match features of the claims with the features disclosed in the cited art in discerning the basis for the Office Action's rejections. Therefore, the Applicant respectfully requests that in any future Office Actions, that the Office

Action identify which features of the cited art correspond to the features of the claims. In particular, the Applicant would appreciate the Office Action identifying which features of the prior art correspond to the "first request," "second request," "identifier," and the "association" between the session key and the identifier so that the Applicant is able to better understand the basis of the Office Action's rejections.

As explained below, the Applicant is unable to identify numerous features of the claims in the cited art based merely on the citation of different paragraphs as in the present Office Action. The Applicant notes that not just the cited paragraphs of the cited prior art references were reviewed in trying to understand the basis of the Office Action's rejections, but rather that the Applicant reviewed the entirety of the references to determine whether the references discloses elements that correspond to the claimed features elsewhere. Nevertheless, the Applicant was still unable to find any discloses of the prior art corresponding to many of the features of Claim 1, as described in detail below.

The Office Action states that *Trostle* discloses "receiving, from a first node, a first request to store an encryption key, wherein the first request includes an identifier, and wherein the first node uses the encryption key to encrypt data that is multicast with the identifier to a plurality of second nodes; [0050][0053]." However, paragraph [0050] discusses the problem of key substitution during transmission and the use of a trusted intermediary, such as a KDC, to distribute stored secret keys to multicast members. *Trostle* explains that the KDC encrypts the secret keys with keys protected by the respective member's secret keys (e.g., by encrypting the secret keys with each members public key, thereby allowing the member to decrypt the secret key using the member's private secret key). But nowhere in paragraph [0050] can the Applicant identify "a first request...to store an encryption key," little less that such a request includes an "identifier."

Paragraph [0053] describes the KDC 111 authenticating members of the multicast, that the members obtain dynamic session keys from the KDC, and that either the KDC or the member nodes generate a dynamic group key. But yet again, the Applicant fails to see anything about "a first request...to store an encryption key," little less that such a request includes an "identifier." As noted above, the Applicant respectfully requests that any future Office Action identify what elements or parts of paragraphs [0050] and [0053] the Office Action is relying upon as corresponding to the "first request...to store an encryption key" and

the "identifier" that is included in that request as the Applicant is unable to identify anything that would reasonably be taken as corresponding to those features of Claim 1.

The Office Action also states that *Trostle* discloses "in response to the first request, storing the encryption key; [0049]." But paragraph [0049] describes basic public key encryption in which public keys are published in a database that can be accessed to retrieve the public key of a participant to who a message is to be sent. While the database certainly stores public keys, this step of Claim 1 is not the storing of a public key but rather of the "encryption key" that is both used by the first node to encrypt data that is multicast (see the first step of Claim 1) and used by the at least one second node for decrypting the encrypted data (see the last step of Claim 1). Thus, the "encryption key" of Claim 1 is used for both encryption and decryption of the data sent in the multicast, whereas the "public keys" stored in the database described in paragraph [0050] are only used for encrypting messages (since the private keys are used for decryption). Furthermore, the public keys are not described as being used for a multicast but only to communicate with a particular node, which is a "unicast" (e.g., a transmission from one node to another) not a multicast (e.g., a transmission from one node to two or more nodes) as in Claim 1.

The Office Action states that *Trostle* discloses "in response to the first request, creating and storing an association between the encryption key and the identifier; [0028][0049][0050]." Paragraph [0050] and it's discussion of key distribution by a KDC was addressed above, and as noted therein, the Applicant fails to see anything in paragraph [0050] that would correspond to an "identifier." Similarly, the Applicant fails to see anything in paragraph [0050] that corresponds to "an association between the encryption key and the identifier." As for paragraph [0049], the discussion of a database of public keys that allow members to securely communicate describes nothing about the "encryption key" of Claim 1, little less an "identifier" as featured in Claim 1, and little less anything about an "association" between that encryption key and the identifier that is both created and stored in response to the first request to store the encryption key.

Finally, paragraph [0028] describes registering subscribers and publishers with an event server that performs an authorization check to ensure that only authorized publishers produce certain events and that only authorized subscribers receiver those certain events. The paragraph continues in describing that if the publishes and subscribers are authorized, the

group session key is generated for establishing the multicast group and that the session key is distributed to subscribers via a message with a prescribed format, along with determining whether the correct key version is used and updating the group session key, if necessary, with reregistering the subscribers.

As best understood by the Applicant, it appears that the Office Action is equating the identifier to the "key version" referred to in paragraph [0028]. Yet if that is the case, the Applicant fails to see anything about a "key version" in the portions of *Trostle* cited for the other steps of Claim 1 that include the "identifier." For example, the Applicant fails to see anything about a "key version" in the paragraphs relied upon in the Office Action as allegedly disclosing the first step of Claim 1 that features the "identifier" being included in the request to store the encryption key. Finally, the Applicant still fails to see anything in paragraph [0028] that corresponds to an "association" between the group session key and the key version, little less that such an association is *both* created and stored ***in response to the first request*** to store the encryption key.

The Office Action also states that *Trostle* discloses "receiving, from at least one second node of the plurality of second nodes, a second request to obtain the encryption key, wherein the second request includes the identifier; [0028][0048]." Paragraph [0028] is discussed above, and based on the same understanding that the key version is the identifier, the Applicant still fails to see anything in paragraph [0028] that describes a request for the encryption key based on the key version. Regarding paragraph [0048], that portion of *Trostle* describes how a directory is used to distribute and update group session keys with the use of a group controller that is implemented as an event server. *Trostle* explains that the event server manages the public and private keys for all the subscribers and publishers and is integrated with the multi-master directory. Yet that still says nothing about a node requesting the encryption key based on the identifier as in Claim 1. As best understood by the Applicant, the group session key is distributed automatically to the publishers and subscribers as part of the authentication process, which is address above with regards to paragraph [0028]. Therefore, neither the subscribers or publishers make a request to obtain the encryption key, little less a request that includes the identifier included in the previous request to store the encryption key.

The Office Action states that *Trostle* discloses "in response to the second request, based on the identifier included in the second request and the association between the

encryption key and the identifier, retrieving the encryption key; [0028] and [0049]." Both paragraphs [0028] and [0049] are addressed above, and again, the Applicant fails to see anything about an association between the group session key and the key version or a request to obtain the group session key that includes the key version, little less that a particular group session key is retrieved based on a particular key version. Rather, *Trostle* explains in paragraph [0028] that the key version is merely checked to see if it is correct, and if not, the group session key is updated by the event server and subscribers selectively reregistered. Thus, *Trostle* does not allow for subscribers to request particular group session keys based on the version (e.g., what the Office Action is apparently equating to the identifier in the "creating and storing" step of Claim 1). And in *Trostle's* approach, if the key version is wrong, no group session key is retrieved, but rather a new group session key is generate as part of the "updating" process and presumably distributed to the subscribers automatically as part of the reregistering of the subscribers and not in response to the subscribers requesting the session key based on the correct key version. Thus, the Applicant yet again does not see anything in *Trostle* corresponding to this step of Claim 1.

Finally, the Office Action states that *Trostle* discloses "in response to the second request, sending the encryption key to the at least one second node for use in decrypting the encrypted data. [0050]" As addressed above, paragraph [0050] describes that a trusted intermediary is used to distribute stored secret keys via public key encryption using the public keys of the receiving multicast member. Yet the final step of Claim 1 is that sending the encryption key is "in response to the second request." But as discussed above, the Applicant fails to see either in paragraph [0050] or any of the other cited paragraphs for Claim 1 such a request to obtain the encryption key and as explained above, the Applicant understands *Trostle* as distribution the group session keys upon authenticating the subscribers and publishers without either having to request the group session key via an identifier that is associated with the group session key, as in the approach of Claim 1.

(4) CONCLUSION OF DISCUSSION OF CLAIM 1 AND *TROSTLE*

As best understood by the Applicant, *Trostle's* invention is directed to the use of a multi-master directory to facilitate a scalable architecture for managing multicasts that is not susceptible to the single point of failure and bottleneck issues discussed in the Background

section of *Trostle*. However, other than the use of the multi-master directory, the distribution of group session keys in *Trostle* is conventional in that the group session keys are generated by the KDC, and then the KDC distributes the group session keys to the member nodes as part of authorization or registration by the KDC of the subscribers and publishers.

For example, paragraph [0112] of *Trostle* describes that upon authorizing a principal, the event server generates a group session key that is encapsulated in an LDAP message that is distributed to the subscribers. Similarly, as described in paragraphs [0114] and [0115], when a new group session key is needed (e.g., the group session key must be updated), the event service node creates the new group session key (paragraph [0114]), and then the event server sends a message to the subscribers to reregister, thereby distributing the new group session key automatically via the re-registration process. Thus, in *Trostle's* approach, the subscribers are not sending a request to the event server to obtain the group session key since the group session keys are automatically distributed as part of registering. Therefore, *Trostle's* approach also fails to disclose sending a request to obtain the group session key that includes an identifier for which an association with the group session key is created and stored by the KDC in response to yet another request to store that group session key, which is a fundamental difference between the approach of *Trostle* and Claim 1.

As best understood by the Applicant, the Office Action's rejection of Claim 1 is based on equating the key version to the "identifier" of Claim 1, but if that were the case, *Trostle* would need to disclose the KDC receiving a request to store a group session key in which the request includes the key version number, the KDC creating and storing an association between the group session key and the key version in response to the request to store the encryption key (hence, that association would not exist prior to the request), and the KDC receiving another request from another node in which the other request includes the key version so that the KDC can retrieve the group session key based on the association between the group session key and the key version. But nowhere in either the cited portions of *Trostle* or any other portion of *Trostle* can the Applicant find such requests and such uses of the key version, little less the creation and storing of an association between the group session key and key version. In fact, in the portions of *Trostle* cited in the Office Action for the steps of receiving the first and second requests, there is no mention of the key version at all.

Because *Trostle* fails to disclose, teach, suggest, or in any way render obvious "**receiving**, from a first node, **a first request** ***to store an encryption key***, wherein the first request includes an ***identifier***...," "in response to the first request, ... **creating and storing** an association **between the** ***encryption key*** **and the** ***identifier***," "**receiving**, from at least one second node of the plurality of second nodes, **a second request** ***to obtain the encryption key***, wherein the second request includes the ***identifier***," and "in response to the second request, **based on the** ***identifier*** included in the second request **and the** ***association*** between the encryption key and the identifier, retrieving the encryption key," the Applicant respectfully submits that, for at least the reasons stated above, Claim 1 is allowable over the art of record and is in condition for allowance.

B. CLAIMS 21-29

Claims 21-29 contain features that are either the same as or similar to those described above with respect to Claim 1. For example, Claims 24, 26, and 28 all feature "**receiving**, from a first node, **a first request** ***to store an encryption key***, wherein the first request includes an ***identifier***...," "in response to the first request, ... **creating and storing** an association **between the** ***encryption key*** **and the** ***identifier***," "**receiving**, from at least one second node of the plurality of second nodes, **a second request** ***to obtain the encryption key***, wherein the second request includes the ***identifier***," and "in response to the second request, **based on the** ***identifier*** included in the second request **and the** ***association*** between the encryption key and the identifier, retrieving the encryption key,", which are the same as in Claim 1.

As another example, Claims 21, 25, 27, and 29 all feature "sending an encryption key and an identifier that is associated with the encryption key to an authoritative node that stores the encryption key and identifier and that creates and stores an association between the encryption the encryption key and the identifier" and "wherein the one or more receiving nodes use the identifier to retrieve the encryption key from the authoritative node," which are similar to Claim 1.

As yet another example, Claim 22 features "receiving from an originating node a multicast that includes encrypted data and an identifier," "identifying the identifier from the multicast," "sending a request that includes the identifier to an authoritative node for an

encryption key," and "in response to the request to the authoritative node, receiving the encryption key," which are similar to Claim 1.

Finally, Claim 23 features "receiving, at the certificate authority from a first router that acts as a multicast originator, a first request to register an encryption key, wherein the first request includes a multicast session identifier," "in response to the first request, the certificate authority creating and storing a multicast session certificate that includes the encryption key, the multicast session identifier," "receiving, at the certificate authority from at least a particular second router of the plurality of second routers, a second request to obtain the encryption key, wherein the second request includes the multicast session identifier, "in response to the second request,... based on the multicast session identifier included in the second request and the multicast session certificate, the certificate authority retrieving the encryption key," which are similar to Claim 1.

Therefore, based on at least the reasons stated above with respect to Claim 1, the Applicant respectfully submits that Claims 21-29 are allowable over the art of record and are in condition for allowance.

C. CLAIMS 2, 6, 9, 11-12, 15, 17, AND 30-45

Claims 2, 6, 9, 11-12, 15, 17, and 20 are dependent upon Claim 1, Claims 30-37 are dependent upon Claim 26, and Claims 38-45 are dependent upon Claim 28. Each of Claims 2, 6, 9, 11-12, 15, 17, and 30-45 is therefore allowable for the reasons given above for Claims 1, 26, and 28. In addition, each of Claims 2, 6, 9, 11-12, 15, 17, and 30-45 introduces one or more additional limitations that independently render it patentable. However, due to the fundamental differences already identified, to expedite the positive resolution of this case a separate discussion of those limitations is not included at this time. Therefore, it is respectfully submitted that Claims 2, 6, 9, 11-12, 15, 17, and 30-45 are allowable for the reasons given above with respect to Claims 1, 26, and 28.

D. EXCLUSION OF *TROSTLE* UNDER 103(c) IN THE REJECTIONS OF CLAIMS 6, 9, 11, AND 23

Claims 6, 9, 11, and 23 have been rejected under 103(a) for allegedly being obvious based on *Trostle* in view of either *Hsu* (Claim 6) or *Turtiainen* (Claims 9, 11, and 23).

However, under 35 U.S.C. 103(c)(1): "Subject matter developed by another person, which qualifies as prior art only under one or more of subsections (e), (f), and (g) of section 102 of this title, shall not preclude patentability under this section where the subject matter and the claimed invention were, at the time the claimed invention was made, owned by the same person or subject to an obligation of assignment to the same person."

Pursuant to MPEP 702.02(l)(2)(II), the Applicant provides the following statement of common ownership:

> **Application 09/996,948 and the subject matter of U.S. Patent Application Publication 2005/0097317 A1 were, at the time the invention of Application 09/996,948 was made, owned by Cisco Technology, Inc.**

Because *Trostle* cannot be used in a 103(a) rejection per 103(c) and because none of Claims 6, 9, 11, and 23 are disclosed, taught, suggested, or obvious in view of either *Hsu* or *Turtiainen*, either along or in combination, the Applicant respectfully submits that Claims 6, 9, 11, and 23 are allowable over the prior art.

CONCLUSION

The Applicant believes that all issues raised in the Office Action have been addressed and that allowance of the pending claims is appropriate. After entry of the amendments, further examination on the merits is respectfully requested.

The Examiner is respectfully requested to contact the undersigned by telephone if it is believed that such contact would further the examination of the present application.

For the reasons set forth above, it is respectfully submitted that all of the pending claims are now in condition for allowance. Therefore, the issuance of a formal Notice of Allowance is believed next in order, and that action is most earnestly solicited.

To the extent necessary to make this reply timely filed, the Applicant petitions for an extension of time under 37 C.F.R. § 1.136.

If any applicable fee is missing or insufficient, throughout the pendency of this application, the Commissioner is hereby authorized to any applicable fees and to credit any overpayments to our Deposit Account No. 50-1302.

Respectfully submitted,
HICKMAN PALERMO TRUONG & BECKER LLP

Date: January 5, 2006

Craig G. Holmes
Reg. No. 44,770

2055 Gateway Place, Suite 550
San Jose, CA 95110-1089
Telephone: (408) 414-1207
Facsimile: (408) 414-1076

CERTIFICATE OF MAILING

I hereby certify that this correspondence is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Hon. Commissioner for Patents, Mail Stop AMENDMENT, P.O. Box 1450, Alexandria, VA 22313-1450.

on Jan. 5, 2006 by Tracy Reynolds